POL14:

INFORMATION SECURITY POLICY

Rev: 04

HENLEYS MEDICAL SUPPLIES LTD.
Brownfields
Welwyn Garden City
Hertfordshire
AL7 1AN

01707 385226
www.henleysmed.com

1. Policy Statement

Henleys Medical Supplies is committed to respecting the privacy of all customers and employees, and to protecting such data from outside parties. To this end, there are stringent internal procedures which control the processing of sensitive information.

There are safeguards in place to protect cardholder data, privacy, and to ensure compliance with various regulations and laws, along with guarding the future of the organisation.

Company policies are available electronically at all times to internal employees, and externally upon request.

2. Policy

2.1. Scope

The purpose of this policy is to ensure that all information and information systems upon which Henleys Medical Supplies depends are adequately protected to the appropriate level. Henleys Medical Supplies is committed to:

- Regarding information security as a critical issue
- Developing a culture of information security awareness
- Following a balanced information risk strategy based on formal methods for risk assessment, management, and acceptance
- Implementing information security controls which are proportionate to risk
- Achieving individual accountability for compliance with information security policies and supporting procedures.

2.2. Responsibilities

2.2.1. Managing Director

The Managing Director is responsible for monitoring and analysing security alerts and information, with the aid of the IT Manager, and distributing them to the appropriate staff, and for actively administering directory user accounts, including additions, deletions, modifications, and review.

2.2.2. Directors/Senior Management/Managers

All members of the management team are responsible for overseeing their direct staff, and for ensuring the necessary training is completed.

2.2.3. All Employees

All employees have a responsibility for ensuring that Henleys Medical Supplies' systems and data are protected from unauthorised access and improper use.

Employees handling sensitive cardholder data should ensure they:

- Handle both company and cardholder information in a manner that fits with their sensitivity and classification
- Limit personal use of the company's information and telecommunication systems, and ensure it does not interfere with job performance
- Note that the company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems, and network traffic for any purpose
- Do not use email, internet, and other company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing, or illegal

- Do not disclose personnel information unless authorised
- Protect sensitive cardholder information
- Keep passwords and accounts secure
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.
- Do not install unauthorised software or hardware, including modems and wireless access, unless explicit management approval is given
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended
- Report information security incidents without delay.

2.3. Acceptable Use

Management is committed to protecting the employees, partners, and the company from illegal or damaging actions, either knowingly or unknowingly by individuals. As such:

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use
- Employees should take all necessary steps to prevent unauthorised access to confidential data, including card holder data
- Employees shall keep passwords secure. Authorised users are responsible for the security of their passwords and accounts
- All PCs, laptops, and workstations should be secured with a password-protected screensaver or automatic logout feature
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered
- Users should report any suspicious behaviour where any tampering or substitution may be performed
- Information contained on portable computers is especially vulnerable, so special care should be exercised
- Postings by employees from a company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of business duties
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

2.4. Protection of Stored Data

All sensitive cardholder data stored and handled by the company and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by for business reasons must be discarded in a secure and irrecoverable manner.

It is strictly prohibited to store:

- The contents of the payment card magnetic stripe (track data) on any media whatsoever
- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever
- The PIN or the encrypted PIN Block under any circumstance.

2.5. Information Classification

Confidential data	Might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would

	cause severe damage to the Company if disclosed or modified. Confidential data includes cardholder data.
Internal use data	Might include information that the data owner feels should be protected to prevent unauthorised disclosure.
Public data	Is information that may be freely disseminated.

2.6. Access to Sensitive Cardholder Data

All access to sensitive cardholder should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder PAN (Primary Account Number) should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data. This requirement does not apply to the company's copy of the credit card terminal receipt
- Access to sensitive cardholder information such as PAN's, personal information, and business data is restricted to employees that have a legitimate need to view such information. No other employees should have access to this confidential data unless they have a genuine business need
- If cardholder data is shared with a Service Provider (third party) then a list of such Service Providers will be maintained. Henleys Medical Supplies will ensure a written agreement, that includes an acknowledgement, is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess
- Henleys Medical Supplies will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service Provider
- The company will have a process in place to monitor the PCI DSS compliance status of the Service Provider.

2.7. Access Control

- Access control systems are in place to protect the interests of all users of computer systems by providing a safe, secure, and readily accessible environment in which to work.
- Henleys Medical Supplies will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible. Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorisation provided jointly by the system owner and the IT Manager. Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level, even if technical security mechanisms fail or are absent. Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to the Finance Director.
- Access to confidential, restricted, and protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative.
- Access for remote users shall be subject to authorisation by a director. No uncontrolled external access shall be permitted to any network device or networked system.

- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks, and other methods as necessary.

2.8. Physical Security

- Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- A list of devices that accept payment card data should be maintained. The list shall include make, model, and location of the device, and the serial number or a unique identifier of the device. The list shall be updated when devices are added, removed, or relocated.
- POS devices surfaces are periodically inspected to detect tampering or substitution. Personnel using the devices should be trained and aware of handling the POS devices. Personnel using the devices should verify the identity of and any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices. Personnel using the devices should report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management. Strict control is maintained over the storage and accessibility of media
- All computers that store sensitive cardholder data must have a password protected screensaver or automatic logout feature enabled to prevent unauthorised use.

2.8. Protection of Data in Transit

- All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.
- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat, or any other end user technologies. If there is a business justification to send cardholder data via email or by any other mode, then it should be done after authorisation and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, SSL, TLS, IPSEC, etc.).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged, and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

2.9. Creation, Retention and Disposal of Information

- All authorised users of company information storage and processing systems have a responsibility to consider security when creating, using and disposing of information owned by Henleys Medical Supplies.
- All data must be securely disposed of when no longer required, regardless of the media or application type on which it is stored. All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons.

- The company will have processes in place for the destruction of hardcopy (paper) materials, requiring that all hardcopy materials are crosscut shredded, incinerated, or pulped so they cannot be reconstructed.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked *To Be Shredded*. Access to these containers must be restricted.

2.10. Virus Control

- Henleys Medical Supplies will maintain detection and prevention controls to protect against malicious software and unauthorised external access to its networks and systems. It is a disciplinary matter to introduce a virus or take deliberate action to circumvent precautions taken to prevent the introduction of a virus.

2.11. Business Continuity

- Henleys Medical Supplies has approved, and regularly reviews, a business continuity management process aimed at counteracting interruptions to normal company activity and protecting critical processes from the effects of failures or damage to vital services or facilities. See the Business Continuity Policy for further information.

2.12. Information Security Incident Reporting

- All authorised users of company information storage and processing systems should report immediately to the Company for any observed or suspected security incidents where a breach of Company information security policies may have or has occurred, or any information security weaknesses in, or threats to, information processing or storage systems.

3. Review

This policy shall be maintained and reviewed by the Managing Director.

Danielle Henley, Managing Director

4. Revision History

Revision	Modified by	Date	Description of Change
01	Andy Cleveland	October 2016	Initial issue.
02	Vikki Patis	April 2017	Annual review.
03	Vikki Patis	April 2018	Annual review. New format.
04	Vikki Patis	December 2020	New format.